NASA Standard Operating Procedure

Network Security Vulnerability Scanning

ITS-SOP-0021 (assigned by the OCIO)
Version: 20051005
Effective Date: 20051005
Expiration Date: 20071005
Responsible Office: OCIO / Chief Information Officer

REVISION RECORD

ITEM NO.	REVISION	DESCRIPTION	DATE

Network Security Vulnerability Scanning

Objective: Despite an organization's efforts to include security measures and implement security controls in a system or application, there is no guarantee that these measures and controls will reliably prevent security incidents over time. Vulnerability scanning is one way to determine how well security measures and controls work at a particular point in time. The results of vulnerability scanning are very sensitive and, if not conducted under strict procedures, may affect the network or system. Vulnerability scanning only determines the vulnerabilities that exist on a computer system without actually circumventing security processes and controls of the system being scanned. This SOP provides guidance on network vulnerability scanning.

Reference: Specific guidance for network security vulnerability scanning can be found in NIST SP 800-42, Guideline on Network Security Testing.

1.0 Implementation

a. NASA shall follow the guidance provided by NIST Special Publication 800-42, Guideline on Network Security Testing.

b. Network vulnerability scanning shall only be conducted with approval by the cognizant Center ITSM.

c. Centers will be responsible for eliminating or mitigating all vulnerabilities on NASA's list of known high risk vulnerabilities. Waivers to this requirement are addressed in section 3 below.

d. Centers shall scan all active and/or registered IP addresses at least twice each quarter. Centers are required to determine the active addresses in use during any given reporting quarter.

e. Scans should be conducted at the beginning of the quarter to obtain a baseline of existing NASA CCITS target vulnerabilities, and at the end of the quarter to assess vulnerability mitigation or elimination efforts.

f. All unscanned devices with active IP addresses shall be tracked and scanned prior to the end of the reporting quarter.

g. Devices that have not been scanned by the end of the quarter should be disconnected from the network, and only re-connected once they have been scanned.

h. Any device associated with an IP address that continues to exhibit vulnerabilities identified during the baseline scan should be disconnected from the network and only reconnected once the vulnerability has been identified and eliminated or mitigated as determined by the Center CIO and ITSM.

i. Each Center shall submit a quarterly report to the NASA Incident Response Center (NASIRC). Centers should denote the subset of vulnerabilities that have been eliminated or mitigated or that have received risk acceptance approval by the Center CIO.

j. For systems with a given vulnerability for which no mitigation strategies are available, the line manager can seek a risk acceptance waiver given the Center CIO's written approval.

k. All mitigation strategies and risk acceptance shall be documented, approved by a government line manager, and concurred on by the Center ITSM, with a copy kept on file with the Center Chief Information Officer (CIO).

l. Mitigation efforts should begin at the host level and move outward through a Center's defenses all the way to the Center's perimeter firewall.

m. All Center CIOs shall report their scanning results at the end of each quarter.

2.0 Data Sensitivity

a. Results from network vulnerability scanning shall be considered ACI or SBU information and will be handled and protected accordingly.

3.0 Waivers

a. Network vulnerability scanning, as part of our quarterly metric reporting is key to ensuring compliance with Federal regulations as well as effectively managing NASA's IT security program. However, extenuating circumstances can, at times, interfere with a Center's ability to meet NASA's IT security metrics.

(1). Obstacles to meeting the intent of IT security metrics stem from two causes -- systemic and temporary. Both systemic (e.g., artifacts of a Centers infrastructure) and temporary (e.g., transitory tests/programs -- return to flight) can impeded meeting the intent of the IT security metrics.

(2). In both these cases, the Center CIO should submit a letter to the NASA OCIO describing the specific requirement(s) called forth in the metric letter that cannot be met. Centers should comment on plans in place to fix the problem and include a schedule that highlights milestones necessary to comply with the metric.

(3). Once a waiver is approved by the NASA CIO, Centers should include a brief explanation of the approved waiver and how it affects Center reporting with each quarterly report.

S. Scott Santiago

10/5/2005

S. Scott Santiago
Deputy Chief Information Officer
Information Technology Security

Date